ABSTRACT

A random number generator comprising a plurality of pseudo random number generating units that can respectively output random numbers in specified pseudo random number systems, an output random number generating unit that generates output random numbers based on outputs from a plurality of pseudo random number generating units, a physical random number generator that generates physical random numbers, and a switching unit for switching between the necessity and the non-necessity of updating output values from pseudo random number generating units based on physical random numbers generated by the physical random number generator. Based on which pseudo random number system an output random number is generated is randomly switched based on a physical random number, making it very difficult to predict a random number compared with a conventional one.